

COMMUNICATION SYSTEM BETWEEN SERVICE SERVER AND SERVICE CLIENT

Japanese Patent No. 3224784

Patent number: JP11296595

Publication date: 1999-10-29

Inventor: YOOKU SHION CHIN

Applicant: INTERNATL BUSINESS MACH CORP <IBM>

Classification:

- International: G06F17/60; G06F13/00; G06F19/00

- european:

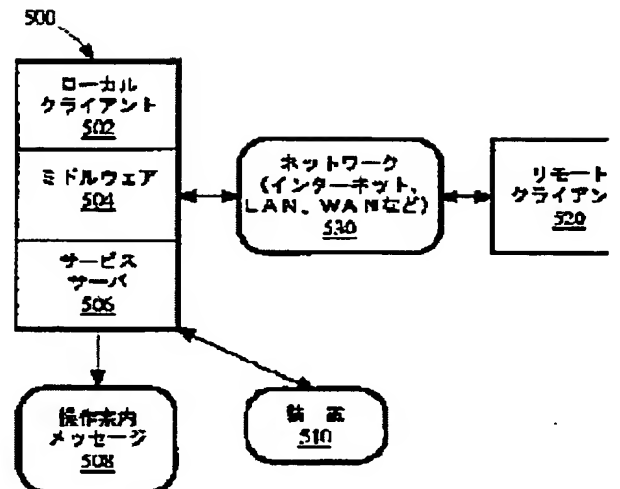
Application number: JP19990005704 19990112

Priority number(s):

Abstract of JP11296595

PROBLEM TO BE SOLVED: To easily adapt the communication system, including the service server and service client, to alterations of devices and services.

SOLUTION: Service specifications issued for the service server 506 are defined on the basis of service specification models as to all services provided in a network 530. The service specification models define the framework of semantics for modeling the message format and flow between the server 506 and clients 502, 520 which are developed independently. This method includes a step for incorporating a client context token into a service request, a step for generating a service server event which can include an exchange token, a step for regenerating a client context token in the service server event, and a step for generating a no-send request service server event which can include the exchange token.



(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

特許第3224784号

(P3224784)

(45)発行日 平成13年11月5日(2001.11.5)

(24)登録日 平成13年8月24日(2001.8.24)

(51)Int.Cl. ⁷	識別記号	P I	
G 0 6 F 17/60	3 2 4	G 0 6 F 17/60	3 2 4
	4 1 0		4 1 0 A
	5 0 2		5 0 2
	Z E C		Z E C
13/00	3 5 7	13/00	3 5 7 Z
請求項の数4(全 25 頁)			

(21)出願番号	特願平11-5704	(73)特許権者	390009531 インターナショナル・ビジネス・マシー ンズ・コーポレーション (INTERNATIONAL BUSI NESS MACHINES COR PORATION アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)
(22)出願日	平成11年1月12日(1999.1.12)	(72)発明者	ヨーク・シオン・チン シンガポール436885 タンジョン・ル ー・ロード 6シー ナンバー02-02
(65)公開番号	特開平11-296595	(74)代理人	100065455 弁理士 山本 仁朗 (外2名)
(43)公開日	平成11年10月29日(1999.10.29)		
審査請求日	平成11年7月29日(1999.7.29)		
(31)優先権主張番号	9 8 0 0 1 3 2 - 4		
(32)優先日	平成10年1月17日(1998.1.17)		
(33)優先権主張国	シンガポール (SG)		
		審査官	岩間 直純
最終頁に続く			

(54)【発明の名称】 ネットワーク内のサービス・サーバと少なくとも1つのサービス・クライアントの間で通信する方法及びシステム

1

(57)【特許請求の範囲】

【請求項1】 ネットワーク内のサービス・サーバと少なくとも1つのサービス・クライアントの間で通信する方法であって、

前記ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された前記サービス・サーバのサービス仕様を発行するステップと、

前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出するステップと、

前記サービス要求にตอบสนองして前記サービス仕様モデルに準拠して定義された送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するか、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するステップとを含む、

2

前記生成するステップが、前記送信請求サービス・サーバ・イベントまたは前記非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込むステップを含む、

前記引き換えクーポンが、サービス要求を受け入れるための前提条件が満たされているかどうかを前記サービス・サーバが後で判定するための前記サービス・サーバからの情報を含む、前記方法、

【請求項2】 前記送信請求サービス・サーバ・イベントにตอบสนองして前記サービス・クライアントが前記引き換えクーポンを含む別のサービス要求を提出するステップをさらに含む、請求項1に記載の方法、

【請求項3】 ネットワーク内のサービス・サーバと少なくとも1つのサービス・クライアントの間で通信するためのシステムであって、

10

前記ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された前記サービス・サーバのサービス仕様を発行する手段と、

前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出する手段と、

前記サービス要求にตอบสนองして前記サービス仕様モデルに準拠して定義された送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するか、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成する手段とを備え、

前記生成する手段が、前記送信請求サービス・サーバ・イベントまたは前記非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込む手段を含み、

前記引き換えクーポンが、サービス要求を受け入れるための前提条件が満たされているかどうかを前記サービス・サーバが後で判定するための前記サービス・サーバからの情報を含む、前記システム。

【請求項4】前記サーバ・イベントにตอบสนองして前記サービス・クライアントが前記引き換えクーポンを含む別のサービス要求を提出する手段をさらに備える、請求項3に記載のシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は公衆ネットワーク内の独立に開発されたサービス・サーバと1つまたは複数の独立に開発されたサービス・クライアントの間の通信、特にサービス・サーバのサービスを定義して発行し、サービス・クライアントからのサービス要求の結果を要求して取得し、サービス・サーバがイベントをサービス・クライアントに個別に通知するための方法、装置、およびシステムに関する。

【0002】

【従来の技術】いくつかの従来のホスト・コンピュータおよび端末構成を図1および図2に示す。同図では各ホスト・コンピュータが1つまたは複数の端末と通信する。ホスト・コンピュータ・アプリケーション・ソフトウェアへのオンライン・アクセスは、キーボード（図示せず）およびディスプレイ・モニタを備えた端末112の使用から始まった。端末112には、ホスト処理コンピュータ110宛のまたはそこからのメッセージとシステム接続された端末装置が動作するための定義済みの固定論理がインストールされている。端末コンピュータ112はホスト・コンピュータ110の入出力端末として用いられる。

【0003】関連するホスト・コンピュータの例としては、UNIXベースのコンピュータおよびメインフレームが含まれる。このようなシステムでは、ホスト・コンピュータ120、130とリモート端末122、132との間のメッセージは、所定のフォーマットおよびプロ

ー（例えばそれぞれASCIIキーストロークとIBM3270データストリームおよびフロー）に準拠することが必要とされる。ホスト・コンピュータ120、130は端末122、132のキーボードからの入力を受信して端末122、132のディスプレイ・モニタへ出力を送信する。

【0004】いくつかのビジネス環境では端末142、152として他の装置、例えば現金自動支払機、通帳プリンタなどを使用することも必要とされる。例えば、銀行のメインフレーム140は、現金自動支払機などの非標準装置を備えた自動預金支払機（ATM）142に接続できる。従来から、このような非標準または特殊装置は制御装置のコンピュータにインストールされているソフトウェアによって直接制御されている。このソフトウェアは特殊装置が提供する直接インターフェースに関してプログラムされている。ネットワーク環境では、装置コントローラ・ソフトウェアは通常クライアント・ソフトウェアへのサーバとして動作する。この場合、メインフレーム140とATM142の間の通信は、例えばIBM3624、IBM473X、Diebold912、またはNCR ATMのメッセージ・フォーマットおよびフローを介して実行できる。あるいは、銀行の制御装置150を、通帳プリンタ152など別の非標準装置を備えたブランチャター・パーソナル・コンピュータ（PC）に接続することもできる。この構成はまたソフトウェア固有のメッセージ・フォーマットおよびフローを必要とする。したがって、特別のメッセージ・フォーマットおよびフローがこれらの端末142、152用に定義される。

【0005】この場合、端末キーボードからの入力に加えて、ホスト・コンピュータ140、150は通帳プリンタやカード読取装置などのいくつかの非標準装置からの入力を受信することができる。同様に、端末のディスプレイ装置に加えて、ホスト・コンピュータ140、150はレシート・プリンタ、現金自動支払機などの非標準装置へ出力を送信する。このように、しばしば極めて特殊なデータストリームやフローを必要とする多数の可能な端末装置が一般に利用される。

【0006】さらに、ホスト・コンピュータと端末のこのような構成には、インターネットおよびイントラネットのためのウェブ・サーバ160およびブラウザ・コンピュータ162が含まれる。その場合、多様なブラウザ・アプリケーションを用いてPCからウェブ・サーバにアクセスすることができる。ブラウザPCはhttpメッセージを介してウェブ・サーバ用の入出力端末として動作する。

【0007】要するに、図1および図2に示すシステムのメッセージ・フォーマットおよびフローは、ホスト・コンピュータ・アプリケーションが端末122、132、142、152、162内の装置から入力を受信し

5

そこへ出力を送信することができるように定義される。したがって、メッセージ・フォーマットおよびフローは各端末の装置の個々の選択と各装置の特性に極めて特有である。例えば、ホスト・コンピュータは、ATMの非標準装置に前もって挿入されている銀行カードなどの磁気ストライプ上に符号化される、磁気トラック・データを含むフィールドを備えたメッセージを送信することができる。

【0008】このようなホスト・コンピュータおよび端末の既存のメッセージ・フォーマットおよびフローは、新しい装置が端末で使用できるようになったとき、それをサポートするためにしばしば拡張しなければならない。このように、メッセージ・フォーマットおよびフローは多様で複雑なだけでなく、新しい端末装置に適用しなければならないことが多い。

【0009】また、メッセージ・フォーマットは、人間のユーザおよびメッセージのソースを認証するためのフィールドを含むこともできる。例えば、これらのフィールドは、暗号化された個人識別番号(PIN)およびメッセージ認証ダイジェストをそれぞれ必要とすることがある。メッセージ・フォーマット内のこのようなフィールドは、メッセージの違法な盗聴および改竄を防止するためにオンライン・アクセスが機密である場合に必要になることがある。

【0010】複数の組織にまたがって端末コンピュータを共用するために、メッセージを図3に示すような組織間のホスト・コンピュータのために定義できる。これらのメッセージも、ネットワーク204、214、224の端末、それぞれの端末ネットワークのホスト処理コンピュータ202、212、222、および他の組織のホスト・コンピュータ(例えばANSI X9.2)の間で分散される定義された機能に特有である。

【0011】組織間ホスト・コンピュータ・メッセージは他の組織(例えば電子資金転送用のSWIFT)へのサービス提供のためにも定義できる。このようなシステムの例を図4に示す。図では、ホスト処理コンピュータ302、312、322が相互の通信用に構成されている。このような組織間メッセージは装置依存ではなく、組織間データ(例えば資金)転送の目的に特有である。例えば、いくつかの大手の製造業者および小売業者はデータを交換するために用いる構造化データ・フォーマットである電子データ交換(EDI)を用いる。

【0012】端末がより強力になり処理能力が増すにつれて、サーバとしてパッケージ化されたより多くの機能を提供し、従来のメインフレーム・コンピュータまたは別のコンピュータに富駐するクライアントへサービスを提供する。クライアント・サーバ技術の進歩により、サーバ機能は直接装置動作のレベルにある必要がなく、複数の装置または装置あたり複数の動作を含むより高次のレベルにあってもよいようになっている。このことは、

6

かなりの処理能力を備えたホスト・コンピュータであるクライアントおよびサーバ・コンピュータでは自明である。

【0013】この状況は、サービス要求元(すなわち「クライアント」)およびサービス・サーバの動作が極めて特殊なメッセージ・フォーマットおよびフローにより密結合された状況である。メッセージ・フォーマットおよびフローは、サーバが提供しようとするサービスに特有である。例えば、サービス要求元すなわちクライアントは、図2の銀行のメインフレーム・コンピュータ・アプリケーション140であり、サービス・サーバはATM142の内蔵ソフトウェアであり、銀行のメインフレーム・アプリケーションがATMの現金自動支払機のサービスを要求する。

【0014】サービス要求元とサービス・サーバの間のメッセージのフローおよびフォーマットは通信レイヤとは別個に定義される。さらに、メッセージは同じコンピュータ上で走っているクライアントとサーバの間を流れることもできる。例えば、メッセージはアプリケーション・プログラム・インターフェース(API)呼出したローカル・ソケット・メッセージを介することもできる。提供されるサービスが変わるとき、クライアント側およびサーバ側のソフトウェアの同期状態を維持するためにこれらを同時に更新する必要がある場合が極めて多い。

【0015】クライアントには、そのクライアントがサーバによって提供されたサービス・セットを使用するための認証を受けた期限内のみこのサービス・セットへのアクセスが提供される。サービス呼出しのシーケンスもサービスの性質およびサービスの提供方法と密に結合していることがある。例えば、トランザクション状況メッセージは、端末でのトランザクション実行のためのトランザクション許可がホスト・コンピュータから受信された後で初めて、端末からホスト・コンピュータへ送信できる。

【0016】簡素な管理用ワークステーションに寄せる企業の関心から、アプリケーション・サーバからアプリケーション(例えばウェブ・ページ、Javaアプレット)をロードしてサーバ上でアプリケーションを実行するネットワーク・コンピュータが生まれた。そのようなネットワーク・コンピュータは、サーバ上で実行されるWindowsアプリケーションのためのリモート・ユーザ・インターフェースを提供する。明確なPC構成は、アプリケーション・サーバとは別個に実行できる。しかしこの手法はPCに接続される非標準装置に対応できない。

【0017】

【発明が解決しようとする課題】本発明の目的は、サービス・サーバおよびサービス・クライアントを含む通信システムにおいて装置やサービスの変更に対応で

きるようにすることにある。

【0018】

【課題を解決するための手段】本発明の第1の態様によれば、ネットワーク内のサービス・サーバと少なくとも1つのサービス・クライアントの間で通信する方法であって、ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された、サービス・サーバのサービス仕様を発行するステップと、前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出するステップと、前記サービス仕様モデルに準拠して定義されたサービス・サーバ・イベントを前記サービス・サーバによって生成するステップとを含む通信方法が提供される。

【0019】サービス仕様モデルは、互いに独立に開発されたサービス・サーバとサービス・クライアントの間のメッセージ・フォーマットおよびフローをモデル化するためのセマンティクスの枠組みを定義することが好ましい。

【0020】この方法は、クライアント・コンテキスト・トークンをサービス要求に組み込むステップをも含むことが好ましい。またこの方法は、サービス要求に回答して送信請求サービス・サーバ・イベントをサービス・サーバによって生成するステップ、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するステップを含むことができる。さらに、この方法は、送信請求サービス・サーバ・イベント内のクライアント・コンテキスト・トークンを再生するステップを含むこともできる。

【0021】この方法は、送信請求サービス・サーバ・イベントまたは非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込むステップを含むことが好ましい。引き換えクーポンは、サービス要求を別のサービス要求に関連づける。送信請求サービス・サーバ・イベントからの情報を含む。引き換えクーポンは、別のサービス要求を受け入れるための1つまたは複数の前提条件が満たされているかどうかをサービス・サーバが後で判定するためのサービス・サーバからの情報を含むことができる。オプションで、1つまたは複数の前提条件は、一組のサービス・サーバ・イベントと、1つまたは複数の以前のサービス・サーバ・イベントからの累計マイルージ・ポイントとからなるグループのうち少なくとも1つを含む。ただし、サービス・サーバによる前記別のサービス要求の受け入れが生ずるのは、サービス・クライアントのために前者の一組のサービス・サーバ・イベントのうち少なくとも1つが事前に生起している場合である。また、後者の累計マイルージ・ポイントは、サービス・サーバがその数量でリセットできる。すなわち、引き換えクーポンとは、サービス・サーバによって提供される情報を含む、サーバ・コンテキスト・トークンを表すものである。この情報により、サービス・サーバは、サービス要求のコンテキストを判定し、このコン

テキストが累積した価値(例えば、累計マイルージ・ポイント)を判定し、その完全性を検査することができる。累積した価値が一定値に達すると、サービス・クライアントは、それに見合った何らかの権利に引き換えることができる。

【0022】この方法は、サーバ・イベントに応じてサービス・クライアントが引き換えクーポンを含む別のサービス要求を提出するステップをさらに含むことが好ましい。サービス・サーバは、別のサービス要求の引き換えクーポンを用いて別のサービス要求を処理するクライアント・コンテキストを決定することができる。

【0023】オプションとして、この方法は、サービス・サーバで実行されるステップとして、サポートされるサービスおよびサービス・サーバの対応するサービス仕様に関してサービス要求を検証(validate)するステップと、サービス・クライアントを確認または認証するステップと、引き換えクーポンを含むサービス・サーバ要求メッセージを確認または認証するステップとからなるグループのうち少なくとも1つをさらに含むことができる。また、サービス・クライアントによるこの方法の実行は、オプションとして、サービス・クライアントがサービス・サーバ・イベントを確認するステップと、サービス・サーバを確認または認証するステップと、クライアント・コンテキスト・トークンを確認または認証するステップとからなるグループのうち少なくとも1つを含むことができる。

【0024】オプションとして、サービス・クライアントは、サービス・サーバを実装するコンピュータ・システム内で実装される。これはコンピュータ・システムにダウンロードされコンピュータ・システムによって実行されるアプリケーション・ソフトウェアを用いて行うことができる。

【0025】本発明の第2の態様によれば、ネットワーク内のサービス・サーバと少なくとも1つのサービス・クライアントの間で通信するためのシステムであって、ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された、サービス・サーバのサービス仕様を発行する手段と、サービス仕様モデルに準拠して定義されたサービス要求をサービス・クライアントによって提出する手段と、前記サービス仕様モデルに準拠して定義されたサービス・サーバ・イベントを前記サービス・サーバによって生成する手段とを備えるシステムが提供される。

【0026】

【0027】

【発明の実施の形態】本発明は、ネットワーク化された環境内のサービス・サーバが提供するサービスを定義し、発行し、サービス要求の結果を要求して取得し、サービス・サーバ・イベントの非同期の非送信請求通知を

行う方法、装置およびシステムに関する。本発明の好ましい実施形態は、ネットワーク化された環境の独立に開発されたサービス・クライアントとサービス・サーバの間のメッセージ・フォーマットおよびフローを、サービス・クライアントおよびサービス・サーバ・ソフトウェアの開発者の間での最小限の同期調整によって効率よくモデル化できる、簡単な仕様のセマンティクス的一般的な枠組みを提供する。これは、サービス・サーバの既存のサービスを阻害することなく新しいサービスの導入を可能にし、またネットワーク・コンピュータのオープンで柔軟な構成の基礎を形成するのに使用され得る。個々のサービスはダウンロードされたクライアント・ソフトウェア（例えばJavaアプレット、ActiveXオブジェクトなど）またはリモート・コンピュータで実行されるアプリケーションであり、ネットワーク・コンピュータの構成はキーボード、ディスプレイ、マウス、スマート・カード読取装置などの標準装置に限定されない。好ましい実施形態で開発される手法は、各サービス・サーバがそのサービス仕様を独立に定義して発行することに基いている。これらの仕様は、管理組織によって管理されないコンピュータの動作を構成するのに使用されるデータの基礎を形成することができる。例えば、この仕様はローカルのスマート・カード・チップまたはリモート・コンピュータからロードできる。好ましい実施形態のシステムは、メッセージ・フォーマットおよびフローを定義しない。メッセージ・フォーマットおよびフローの実際の定義は、サービス仕様およびそのイベント・シーケンスに密接に関連しているか、またはそれらにマップする。

【0028】ネットワーク化環境の概要

ネットワークに接続されたどのコンピュータも本発明の好ましい実施形態に従って公衆ネットワーク内の他の任意のコンピュータ（すなわちサービス・クライアント）に対してサービス・サーバとして動作できる環境を図5に示す。このネットワーク化環境の例では、ATM420およびキオスク422が設置され、公衆ネットワーク400、好ましくはインターネットまたはイントラネットを介してサービス局418によって運用される。サービス局418は、そのキオスクのサービスを複数の異なる加入者組織の消費者に提供する。加入者組織はキオスクとの間で用いる専用のアプリケーション・ソフトウェアを独立に開発して維持する。アプリケーション・ソフトウェアは、加入者のウェブ・サイトを介して提供されるWWWアプリケーションでもよい。この例のサービス局418はATMに現金を補給し、必要があればいつでもATMを修理する責任がある。銀行428などの加入者組織の顧客はATM420から現金を取得することができる。さらに、旅行代理店432など他の加入者組織の顧客もキオスク422を使って旅行のチケットを購入できる。

【0029】サービス局418自体が、消費者がキオスクを操作する手助けをする過程で消費者のためにキオスク装置を操作するサービス要求を出すコール・センター・エージェントを有することができる。このシナリオでは、サービス局418が運用するコンピュータによって実施されるキオスク・ネットワーク・マネージャは、ATM420およびキオスク422へのサービス要求元（クライアント）である。キオスク・ネットワーク・マネージャはこれらの端末420、422へコマンドを送信し、共通処理状況応答（例えばキー同期コマンド）を取得する。ネットワーク・マネージャはまた端末から非送信請求端末状況変更通知を取得する。

【0030】銀行410は、ブランチ・ローカル・エリア・ネットワーク（LAN）424、そのテラ・PC、および接続されたテラ装置（例えば追帳プリンタなど）を所有する。ブランチLAN424、テラ・PC、および接続されたテラ装置は、銀行410、および例えば銀行410が買収したばかりの銀行428の両方の顧客へサービスを提供する。

【0031】スタチュトリ・ボード（statutory board）426は、そのサービス・クライアントである輸出会社412へ公衆ネットワーク400を介して関税処理サービスも提供するサービス・サーバとして動作できる。

【0032】ホームPC430は、ホームPC430へのサービス・サーバである銀行410からPCオペレータの口座残高に基づいて購入クーポンを取得するサービス・クライアントでもよい。購入クーポンはホリディ・パッケージを購入するために公衆ネットワーク400を介して、サービス・サーバとして機能する旅行代理店432へ渡される。クーポンはその後サービス・クライアントとして機能する旅行代理店432によって適切な資金を引き出すために銀行410へ提出される。

【0033】キオスク422は銀行428のウェブ・サイトからウェブ・ページを取り出すこともできる。ウェブ・ページは銀行428の顧客サービスの一環として銀行428のためにキオスク422上でローカルに実行可能なJavaアプレットを備えることができる。

【0034】ネットワーク・コンピュータ416は、アプリケーション・サーバ414からアプリケーション・ソフトウェア（例えばWWWページおよびJavaアプレット）をロードして実行し、サーバ414が実行するWindowsアプリケーションのためのリモート・ユーザ・インターフェースを提供することができる。キーボード、マウス、ディスプレイ・モニタ、スマート・カード読取装置などの標準PC装置に加えて、通帳プリンタを含むその他の非標準装置もネットワーク・コンピュータ416に接続することができる。

【0035】前述のネットワーク化環境の例から理解できるように、多数のさまざまな加入者組織、コンピュー

タ・システム、および非標準装置が公衆ネットワークを介して利用できる。ネットワークに接続されたコンポーネントはそれぞれ他のコンポーネントおよびそれ自体に対してサービス・サーバとしてもサービス・クライアントとしても動作できる。各コンポーネントは専用のメッセージ・フォーマットおよびフローを有することができるため、このようなコンポーネントを使用するクライアントおよびサーバ・ソフトウェアの設計者には可能な組み合わせが無数に存在するという点で重要な課題が提起されている。

【0036】以上のように、公衆ネットワーク環境は、サービス・サーバを利用しようとする個々の組織が開発するクライアント・ソフトウェアの個々の開発者にとって、本出願人が識別した幾多の困難を提起する。

【0037】上記のネットワーク環境が提起する1つの困難は、サービス・クライアントのために個別に開発されたソフトウェアがどの特定のサービス・サーバにもサービスを要求する方法である。クライアント・ソフトウェアの個々の開発者が開発および試験の基準とする、明確で簡潔で曖昧でないサービス仕様モデルが必要である。サービスの定義も異種ネットワーク間で有効であるためにはネットワーク・トランスポートおよびネットワーク・プロトコルから独立している必要がある。この課題に対処するための一般的手法は、サービスおよび各サービスを使用するのに必要な固有のメッセージ・フォーマットおよびシーケンスを発行することである。例えば、ATMの供給業者はその装置に固有のメッセージ・フォーマットおよびフローを提供できる。しかしながら、これにはクライアント・ソフトウェアが各装置に固有の多様なメッセージ・フォーマットおよびフローに対応できることが必要である。サービス・サーバ・ソフトウェアはまた合意された規格に従って、サービス問い合わせメッセージに回答してサービス機能のディスカバリに参加したり、サービス機能公示メッセージを生成したりすることもできる。

【0038】ネットワーク化された環境における別の困難は、サービス・クライアント用の独立に開発されたソフトウェアがサービス・サーバが用いる仕様を満足することをサービス・サーバが検証できなければならないことである。

【0039】さらに別の困難は、クライアント・ソフトウェアによるサービスの「違法な」使用（例えば、消費者がカードを挿入する前にPIN入力要求したり、あるいはサービス・サーバ内のデータベースへの違法な更新を要求する）をどう防止するかである。サービスをできる限り適法である（例えば、リモート・アプリケーションによって実行できないオペレーションへサービスを提供しない）よう定義できる一方で、ある種の「機密」サービスは依然として認証されたサービス・クライアントだけに提供しなければならない。サービス要求は、以

前にサービス・サーバによって生成された「満了」していない一組のサービス・サーバ・イベントの直後に行われるならば、サービス・サーバによって受け入れられる。これには次の例がある。

(a) 現金支払サービス要求は、所定の条件を満たすサービス・クライアントからのみ許される。その条件とは、サービス・クライアントが認証されていて、以前に暗号化PIN入力サービスを成功裏に要求しただけでなく、現金支払要求を受け付ける前にキオスクがタイムアウトにならず且つトランザクションを取り消していないことも必要とする。

(b) PIN入力を求めるサービス要求は、カードが先にキオスクに挿入されサービス要求がカードの妥当性検査のためにホスト・コンピュータへ送信された場合に限って、サービス・クライアントとして動作するホスト・コンピュータから受け入れられる。

【0040】さらに、サービス・サーバが承認された一定の方式で動作するようにすることが必要である。例えば、キオスクで消費者のカードを返却する過程で同じプロンプトが表示され、同じタイムアウト時に消費者はどのサービス・クライアントがサービスの対象であるかにかかわらず同じ消費者対話操作を用いて、カードを確保する前に再度指示される。また、クライアントがカードを（例えばトランザクションを取り消すために）イジェクトできないようにし、なおかつ後でキオスクから現金を引き出せるようにする必要がある。

【0041】さらに別の困難は、各クライアントがサービス・サーバから同時にサービスを受けているサービス要求の複数のスレッドを有し得ることである。各スレッドのサービス要求は相互に関連している。したがって、好ましい実施形態では、サービス・サーバは新しいサービス要求を同じコンテキストに対するものとして以前のサービス要求に関連付けることができなければならない。新しいコンテキストはサービス・サーバ・イベントで開始する。サービス・サーバ・イベントに回答して実行されるサービス要求は、イベントが属するコンテキストの一部である。後続のサービス・サーバ・イベントも同じコンテキストの一部となることができる。

【0042】さらなる困難は、サービス・クライアントが、サービス・サーバからの送信請求サービス・サーバ・イベントを、先にサービス・サーバへ送出されたサーバ要求に回答して生成されるものとして関連付けることができないかもしれないことである。

【0043】別の困難は、所与のコンテキストに対する以前のサービス要求の完了前に、同じサービス・クライアントからの新しいサービス要求を受け入れることができるということである。例えば、これはサービス・クライアントが以前に出したサービス要求の処理を取り消す、同じクライアントからのサービス要求を含む。

【0044】さらに、安全でないネットワークでは、サ

ービス・サーバがサービス・クライアントの識別を認証でき、サービス・クライアントがサービス・サーバの識別を認証でき、サービス・サーバが引き換えクーポンを含むサービス要求メッセージを認証でき、サービス・クライアントがクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを認証でき、サービス・クライアントおよびサービス・サーバがサービス・クライアントとサービス・サーバの間で転送されるデータの選択された部分を暗号化できる必要がある。サービス・サーバの所有者およびサービス・クライアントの所有者は、アプリケーションの機密保護要件によって、また要求される機密保護がすでに他の手段（例えばミドルウェア、イントラネット・ファイアウォール）を介して利用できるかどうかによって、上記の機密保護機能の全部または一部が不要であると決定できる。

【0045】最後に、サービス・サーバがサービス要求をどう処理するかについてのサービス・クライアントの予想が、サービス・サーバが実際にサポートする内容と一致することをサービス・サーバが確認する必要がある。

【0046】本発明の好ましい実施形態はこれらの困難を克服できるか少なくとも緩和できるサービス仕様を提供する。

【0047】好ましい実施形態のサービス・サーバとサービス・クライアント好ましい実施形態によれば、サービス・サーバは装置（例えば現金自動支払機、カード読取装置、キーボードなど）のいかなる動作に関するサービスも提供できる。また、サービス・サーバはオプションで人間の対話操作を必要とし、そのサービスの提供時に案内メッセージの使用を要する。例えば、メインフレーム・コンピュータ上で走るアプリケーションは、サービスの提供時に人間の対話操作を必要としないサービス・サーバの1つの形式である。これとは対照的に、サービス・サーバとして動作するキオスク（例えば図5の422）は、消費者との対話（例えば消費者にキオスクの現金自動支払機420から現金を取り出すよう依頼すること）を必要とするサービス・クライアントとして動作するバックエンドのメインフレーム・アプリケーションが要求するサービスを提供できる。キオスクが提供するサービスがサービス・サーバ側で人間の対話操作を含むこの状況では、キオスク装置を含むサービス・オペレーションは案内画面またはメッセージと連携して行われる必要がある。

【0048】好ましい実施形態によるこのようなサービス・サーバは、サービス・クライアントからのサービス要求に対して1つまたは複数のサービス・サーバ・イベントで応答する。これは装置の非同期動作とネットワークを介して提供される応答メッセージの非同期的な性質に対応する。サービスの実行またはパフォーマンスで復

数のイベントが生成されることがある。したがって、イベントは単一の、複数の、または反復するイベントである。例えば、サービス要求の処理は、それぞれをクライアントがイベントによって通知される必要がある複数のステップを含むことがある。サービスの実行は反復するイベントも生成することがある。例えば、キオスクがあるサービス・クライアントについて銀行カード、クレジットカード、カードその他を受け入れられるようにするサービス要求は、クライアントの顧客によってカードが新たに挿入されるたびに1つのイベントを生成する。

【0049】さらに、サービス・サーバに事前登録された（すなわちオフライン）サービス・クライアントは、サービス・サーバから非送信請求サービス・サーバ・イベントを受信することもできる。例えば、サービス・サーバとして動作するブラウザPCは、サービス・クライアントとして動作するWWWサイトにウェブ・ページをブラウザPCへ送信させる非送信請求サービス・サーバ・イベント（例えばHTTP GET）を送信できる。HTTP GET応答は、ウェブ・ページおよび送信請求入力への提示を求めるブラウザへのサービス要求を表す。ウェブ・サイトまたはサーバは、それ自体を、サービス・クライアントとして動作するブラウザPCからサービス要求（例えばHTTP GET）を受信するサービス・サーバとみなすこともできる。これは、1対のサービス・サーバが相互動作し、個別に他方をサービス・クライアントと見なす、数多くの可能性の1例である。Javaアプレットを含むクライアント・ソフトウェアは、サービス・サーバ・コンピュータで実行するためにダウンロードできる。この場合メッセージはローカルであり、おそらくプロセス間またはスレッド間メッセージである。

【0050】サービス要求およびサービス・サーバ・イベントと共に可変およびコンテキスト依存の情報を提供するデータ要素が引き渡される。これらのデータ要素は、実行可能スクリプト、例えば署名が必要などがあるJavaアプレット、Java Script、HTMLを選ぶことができる。

【0051】図6に好ましい実施形態によるサービス・サーバと1つまたは複数のサービス・クライアントを示す。サービス・サーバ506は、ATMなどの端末500を用いて実施できる。端末500はまた、ネットワーク通信のためのミドルウェア504とオプションとしてローカル・クライアント502を含むことができる。サービス・サーバ506は端末装置に操作案内メッセージ508を提供し、1つまたは複数の端末装置510の動作を制御する。サービス・サーバは端末装置を直接管理し制御する。この例では、リモート（サービス）・クライアント520はサービスに関してインターネット、イントラネット、LAN、ワイド・エリア・ネットワーク（WAN）などのネットワーク530で伝送されるメッ

セージを介してサービス・サーバ506と通信する。ローカル（サービス）・クライアント502はローカルにインストールされたクライアント・アプリケーションまたはリモート・コンピュータ要素（例えば520）からダウンロードされたアプリケーション（例えばJavaアプレット）である。このようなローカル・クライアント502はメッセージまたはアプリケーション・プログラム・インターフェース（API）呼出しを介してサービス・サーバ506と通信する。好ましい実施形態によるサービス仕様規格はクライアント・サーバ間通信のセマンティクスとして用いられ、ネットワーク中心のものである。これはサービス・クライアントとサービス・サーバの間のメッセージ・フォーマットおよびフローを特に定義しない。この図は好ましい実施形態のサービス仕様モデルが適用されるサービス・クライアント、サービス・サーバ、およびネットワーク化環境のブロック図である。

【0052】サービス仕様モデル

以下のサービス仕様モデルは特定の好ましい実施形態の詳細を提供する。ただし、本発明は提示された特定の例に限定されるものではない。逆に、本発明の範囲と精神を逸脱しない限りで、当業者には明らかな修正または変更を本発明に加えることができる。ネットワークのサービス・サーバのサービス仕様を以下にサービス・サーバが提供するサービスごとに説明する。

【0053】表A、B、C、およびDにサービス・サーバのサービス仕様を定義し、発行する方法を詳述する。

【0054】表A：サービス・サーバ仕様

(A) サービス・サーバID：ユニコード名文字列。
 (B) サーバ記述：これによってクライアントによる自動検出と潜在的なクライアントへの広告が可能になる。
 (C) サービス要求メッセージ・タイプおよびサービス・サーバ・イベント・メッセージ・タイプの両方についてデジタル署名を生成するためにサービス・サーバがサポートするアルゴリズム・タイプ。この仕様はサービス・サーバが定義して発行するさまざまな可能なアルゴリズムに関する。これらのアルゴリズムは、さまざまな業界標準アルゴリズムと連携してメッセージ内容を用いるランダム・シーディングのさまざまな組み合わせを使ってメッセージに署名することができる。サービス要求メッセージ内のデジタル署名を生成するのに用いるメッセージ内容は、サービス要求メッセージ内のクライアントIDその他の機密メッセージ要素（例えば引き換えクーポン）を含む必要がある。サービス・サーバ・イベント・メッセージ内のデジタル署名を生成するのに用いるメッセージ内容は、サーバID、サービス要求メッセージからコピーされたクライアント・コンテキスト・トークン（送信請求サービス・サーバ・イベントの場合）、その他のサービス・サーバ・イベント・メッセージ内の機密メッセージ要素を含む必要がある。業界標準

アルゴリズムの例は共通秘密対称鍵を用いるデータ暗号化標準（DES）およびデジタル証明書を用いるRSA公開鍵アルゴリズムである。

(D) サービス要求メッセージ・タイプおよびサービス・サーバ・イベント・メッセージ・タイプの両方の選択されたデータ要素の暗号化のためにサービス・サーバによってサポートされるアルゴリズム・タイプ。この仕様はサービス・サーバが定義して発行するさまざまな可能なアルゴリズムに関する。これらのアルゴリズムはサービス要求メッセージ内の選択されたデータ要素を暗号化するために用いる鍵をシードするサービス要求メッセージの一部として伝送されるランダム・データと、サービス・サーバ・イベント・メッセージ内の選択されたデータ要素を暗号化するためのサービス・サーバ・イベント・メッセージの一部として伝送されるランダム・データを用いることができる。業界標準アルゴリズムの例は共通秘密対称鍵を用いるデータ暗号化標準（DES）およびデジタル証明書を用いるRSA公開鍵アルゴリズムである。

【0055】表B：サポートされた各サービス要求のサービス仕様

(A) サービス要求識別仕様：ネットワークのサービス・サーバ内で一意的なユニコード・サービス名文字列。

(B) サービス要求カテゴリ識別仕様：ネットワークのサービス・サーバ内で一意的なユニコード・サービス名文字列。これによりサービス要求の分類が可能になる。

(C) 下記のいずれかを含む前提サービス要求受け入れモードおよび条件。

1) 満足すべき1つまたは複数の前提セット：これはサービス要求への複数の経路を可能にする。セット内で、前提サーバ・イベントは複数回要求されることがある。前提セットの例は「(A、B)、(A2、D、E)、(C3)」、ただしA、B、C、D、Eはサーバ・イベントID／カテゴリの組み合わせである。第2のセットを用いる場合、サーバ・イベントAは2回要求される。第3のセットを用いる場合、サーバ・イベントCは3回発生する必要がある。引き換えクーポンは最後のCイベントで戻される。

1i) 最小累計イベント・ポイント：これらは以前のサーバ・イベントからの同じクライアントについての同じコンテキストで要求される。引き換えクーポンは十分なポイントに達した最後のイベントで戻される。

D) サービス要求がサービス・サーバからのサービス・サーバ・イベントとは別個にサービス・サーバへ提出できるかどうかに関するブール値。コンテキストの一部でないサービス要求（すなわちサービス・サーバ・イベントに依存しないサービス要求）はここでは真と指定される。この仕様は真の場合、次のリストが適用される。

1) 同時発生するサービス要求ID／カテゴリの組み合わせのリスト：このリストはサービス・サーバがこのサー

ビス要求の処理中に受け入れることができる同じクライアントからのサービス要求を識別するために提供される。例えば、このリストはこのサービス要求をその処理中に取り消すことができるサービス要求のID/カテゴリを含むことができる。

E) 引き換えクーポンが必要かどうかを示すブール値。
F) データ引き数のリスト: 各引き数はサービスが要求する特定の情報を提供し、「データID=値」によって識別される。この仕様はまた提供されないすべての引き数のデフォルト値を示す。これらはクライアントまたはサーバの構成に拘束されないフリー・フォーマット仕様である。データ要素ごとに、データ要素を暗号化するかどうかについてのブール値が提供される。データ要素ごとにそのテキスト記述を設けておけば、自動検出によって有用である。

G) 送信請求サーバ・イベント情報: このサービス要求の処理の結果生成されるイベントのリストを含む。サービスが同期化されていてもその完了は少なくとも1つのイベントで示される。以下にリストするイベントは他のサービス要求の結果として生成できるイベントとしても指定できる。

i) 各イベントは一意的に識別される。サービス要求とその結果であるイベントとを容易に関連付けられるように、サービス要求ID/カテゴリ文字列の組み合わせはイベントID/カテゴリ文字列の組み合わせの一部とすることが推奨される。これはそのイベントが1つの特定のサービス要求だけの結果である場合に重要である。

a) サーバ・イベントIDユニコード文字列: 各サーバ・イベント・カテゴリ内で一意的

b) サーバ・イベント・カテゴリIDユニコード文字列: 送信請求および非送信請求サーバ・イベント・カテゴリの両方についてサーバ内で一意的

i i) 各イベントに関する詳細情報:

a) 記述テキスト: 自動検出に有用

b) 引き換えクーポンがこのイベント・メッセージで利用できるかどうかを示すブール値

c) このイベントで得た累計マイルージ・ポイント(ある場合)

d) 記述テキストの記述: サーバの自動検出に有用

e) サービス・サーバ・イベント・データ項目のリスト。各データ項目はイベントに関する特定の情報を提供し、「データID=値」によって識別される。この仕様はデータ項目のフォーマットを指定しない。データ項目ごとに、ブール値がデータ項目を暗号化するかどうかを示す。データ要素ごとにそのテキスト記述を設けておくと、自動検出によって有用である。

f) 次の4つの値を含むグループの1つからのフラグ:

-新しいコンテキストの開始

-コンテキストの中間

-コンテキストの終り、および

-コンテキストの一部ではないイベント外の値

g) このイベントの受信時にサーバ・クライアントが発行できる1つまたは複数のサービス要求セットのリスト。例えば(A, B), (C, D, E), (F,

F))はサービス要求A, CまたはFがこのイベントを受信するサービス・クライアントから受け入れられることを意味する。サービス要求Aが処理されている間、サービス要求Bをサーバへ発行でき、サービス要求Cが処理されている間、サービス要求DまたはEをサーバへ発行でき、サービス要求Fが処理されている間、別のサービス要求Fをサーバへ発行できる。

i i i) ID文字列および所定の意味を有する標準イベント

a) サービス不明

b) サービス仕様不一致

c) コンテキストがサービス・サーバによって取り消された(例えば、消費者がCANCELキーを押下)

d) コンテキストが同じクライアントからの受け入れられたサービス要求によって取り消された

e) 必要な資源(例えば装置)が利用できない

f) 引き換えクーポンが引き換え済み

g) 引き換えクーポンが無効

h) 引き換えクーポンが期限切れ

i) クライアント認証失敗

j) 引き換えクーポン認証失敗

i v) 未定義の理由による拒否を含む他の非標準イベント・タイプについての情報

a) 再発しているかどうかに関するブール値

b) イベントがサービス要求の処理の終了を示しているかどうかに関するブール値

[0056] 表C: サポートされている各非送信請求サービス・サーバ・イベントのサービス仕様

i) 各サーバ・イベント・カテゴリ内で一意的なサーバ・イベントID

i i) 送信請求および非送信請求サービス・サーバ・イベント・カテゴリのサーバ内で一意的なサーバ・イベント・カテゴリ識別

i i i) 記述テキスト: 自動検出に有用

i v) イベントに関する詳細情報

* 引き換えクーポンがこのイベント・メッセージで利用できるかどうかに関するブール値

* このイベントで得た累計マイルージ・ポイント(ある場合)

* サービス・サーバ・イベント・データ項目のリスト。各データ項目はイベントに関する特定の情報を提供し、「データID=値」によって識別される。この仕様はデータ項目のフォーマットを指定しない。データ項目ごとに、ブール値がデータ項目を暗号化するかどうかを示す。

* 次の4つの値を含むグループの1つからのフラグ: 新しいコンテキストの開始、コンテキストの中間、コンテキストの終り、およびコンテキストの一部ではないイベント外の値

* このイベントの受信時にサーバ・クライアントが発行できる1つまたは複数のサービス要求セットのリスト、(A, B), (C, D, E), (F, F)はサービス要求A, CまたはFがこのイベントを受信するサービス・クライアントから受け入れられることを意味する。サービス要求Aが処理されている間、サービス要求Bをサービス・サーバへ発行でき、サービス要求Cが処理されている間、サービス要求DまたはEをサービス・サーバへ発行でき、サービス要求Fが処理されている間、別のサービス要求Fを発行できる。

【0057】表D: メッセージ・タイプおよび要素のサービス仕様

i) サービス要求メッセージ仕様

a) サービス要求識別

b) サービス要求カテゴリ識別

c) データ引き数のリスト: 各引き数はサービスが要求する特定の情報を提供する。各引き数は「データID=値」によって識別される。

d) サービス仕様概要: これによってサービス・サーバのソフトウェアはクライアントが用いるサービス仕様がサービス・サーバがサポートする内容と一致することを確認することができる。

e) クライアントID

f) クライアント・コンテキスト・トークン (生成された1つまたは複数のサーバ・イベント内でサーバによって再生される)

g) クライアントのためにこのサービス要求が用いる引き換えクーポン。引き換えクーポンは現在のサービス要求がサービス・サーバが所望の状態 (例えば以前のサービス要求に応答する1つまたは複数の以前のサービス・サーバ・イベントの生成) に到達した後で処理されることを確認するためにサービス・サーバが用いることができる。例えば、以前の鍵同期化要求の完了の成功、成功裏の消費者カードの受け入れおよびPIN入力の請求がある。サービス・サーバはまた引き換えクーポンが依然として有効であることを確認する。例えば、サービスがタイムアウトして最後のトランザクションを取り消すことがあり、またはサービス・サーバが再ブートした場合もある。引き換えクーポンには次の2つのソースがある。

* サービス・クライアントからの以前のサービス要求を処理する際に生成された1つまたは複数のサービス・サーバ・イベント。引き換えクーポンはクライアントからの以前のサービス要求への応答で生成されたサーバ・イベントで展される。サービス要求がサービス・サーバ・イベントとは別個に発行されたために引き換えクーポン

ンが利用できない場合、またはサービス要求に通じるサービス・サーバ・イベントが引き換えクーポンを提供しない場合には、この引き換えクーポンは空白である。

* クライアントへの以前の非送信請求サービス・サーバ・イベント。例えば、キオスクでのカード挿入の発生の結果、サービス・サーバ・イベントがカードの確認のためにホストへ送信される。このサービス・サーバ・イベントはホストがPIN入力を請求するためにキオスクへのサービス要求内で用いることができる。

h) サービス・サーバがサービス要求メッセージ (すなわち上記の項目) を認証することを可能にする安全なデジタル署名を生成する際に用いるアルゴリズム・タイプ。サービス・クライアントが使用される認証アルゴリズムを示す。サービス・サーバは、このフィールドの使用が各サービス・クライアントにとって必須であるかどうかを指定され得る。各サービス・クライアントは安全でないネットワークの一部でもよいしそうでなくてもよい。

i) 選択されたデータ要素を暗号化する際に用いるアルゴリズム・タイプ。

j) サービス要求メッセージそれ自体を認証する安全なデジタル署名。これによってサービス・サーバは次の動作が可能になる。

* ソース (すなわちクライアントID) の認証

* サービス要求の改ざん (例えばデータ要素の変更) の検出

* 無許可のクライアントによる引き換えクーポンの違法な記録/再生の検出

デジタル署名の詳細は定義されず、サービス・サーバの所有者の指定に任されている。署名はオプションである。管理が行き届いたイントラネットではこれは不要である。必要な認証はサービス・サーバ506とサービス・クライアント502、520を接続するミドルウェア504によっても提供される。サービス・サーバはこのフィールドの使用が各サービス・クライアントにとって必須であるかどうかを指定され得る。各サービス・クライアントは安全でないネットワークの一部でもよいしそうでなくてもよい。

k) 暗号化に用いる暗号化鍵のランダム・シード。これはサービス・クライアントおよびサービス・サーバの両方だけが知っている固定秘密鍵の下で暗号化されたランダム鍵でもよい。

l) サービス・サーバ・イベント・メッセージ仕様

a) イベント・メッセージが送信請求されているかどうかを示すブール値

b) イベントを起動するサービス要求の識別 (非送信請求の場合は無視)

c) イベントを起動するサービス要求カテゴリの識別

d) サーバID

e) サービス・サーバ・イベントID

f) サービス・サーバ・イベント・カテゴリ
 g) クライアント・コンテキスト・クーポンのコピー
 (非送信請求の場合は無視)
 h) サービス・サーバ・イベント・データ項目のリスト: 各項目はサービスが提供する特定情報を与える。各引き数は「データID=値」によって識別される。
 i) サーバがデジタル署名を生成するのに用いるアルゴリズム・タイプ。サーバは使用する認証アルゴリズムを示す必要がある。
 j) 上にリストしたサービス・サーバ・イベント・メッセージ内容を認証する安全なデジタル署名。これは任意選択である。管理が行き届いたイントラネットではこれは不要である。必要な認証はサーバとクライアントを接続するミドルウェアによっても提供される。これはサービス・クライアントとサービス・サーバ間のビジネス調整契約の一部として構成されるオプションである。
 k) 選択されたデータ要素の暗号化に用いるアルゴリズム・タイプ
 * 送信請求の場合、サービス要求メッセージ内でクライアントによって指定される。
 * 非送信請求の場合、サービス・サーバ内で構成される。
 l) サービス・サーバ・イベント引き換えクーポン。この仕様はクーポンのフォーマットの発行を必要としない。ここにリストする詳細は例にすぎない。これはサービス仕様の一部ではないため、発行する必要がない。クライアントが知る必要があるのは次のサービス要求でこのクーポンを含む必要があるということである。提案される内容はサーバの裁量に任されている。
 * 次のような情報への参照用のコンテキストID:
 -最後のサービス要求のID
 -クーポンが対象とするサービス・クライアントのID
 -同じクライアントについての同じコンテキストの前提サービス要求処理情報。これは例えば、現在のコンテキストについてクライアントのためにサーバによりこれまでの累計されたマイルージ・ポイント、または現在のコンテキストについてクライアントのマイルージを取得するために発生したサーバ・イベントのリストでよい。
 * 以前に生成された引き換えクーポンの再使用を防ぐために必要に応じてサービス・サーバによって日付/時間スタンプと共に生成される乱数。サービス・サーバはこの乱数を以降のサービス要求で用いるランダムに変化するパスワードとして使用できる。
 * サービス・サーバがその裁量で一部または全部を暗号化できる。
 m) 選択されたデータ要素の暗号化のために使用される暗号化鍵のランダム・シード。これはサービス・クライアントおよびサービス・サーバの両方だけが知っている固定秘密鍵の下で暗号化されたランダム鍵でもよい。
 【0058】好ましい実施形態によれば、サービスは図

6に示す関連するサービス・サーバ506がサービス要求を処理する過程およびこのような処理の最後に必要とするすべての操作案内および対話を提供する。サービスを要求しているときはサービス・クライアント・ソフトウェア502、520は同時に操作案内および対話508を提供することはない。これによってサービス・サーバ506は人間のオペレータのために一言した操作案内および対話508を保證することができ。以下のサービス仕様はサービスを提供する過程で必要なすべての操作案内および対話508がサービス内で提供されなくてはならないことを規定する。サービス提供の過程とサービス提供の最後に用いられる操作案内および対話508自体はサービス仕様の一部ではない。操作案内および対話508はLEDによって提供され、ディスプレイ・モニタの表示のみによらなくてもよい。これはオプションであり、サービス・サーバ506の裁量に任される。したがって、サービス・サーバの所有者はサービス・クライアント・ソフトウェア502、520に影響を与えずに操作案内および対話508を変更できる。これはサービス・サーバ506が動作して操作案内および対話508を一言して承認された方式で提供することを保證する手助けをする。サービス・サーバ506はディスプレイ案内および対話の目的を含むサービスを提供できる。実際の表示および対話はサービス・サーバの裁量に任されている。
 【0059】さらに、サービス・サーバ506はサービスの処理中に必要に応じて人間の案内を引き継ぐ能力を必要とする。例えば、サービス・サーバは現金を払い出して消費者に払い出された現金を受け取るよう促しながらクライアントのダウンロードされたJavaアプレットやウェブ・ページからディスプレイ画面を引き継ぐ能力がなくてはならない。これはブラウザ・ウィンドウを最小化または非表示にするサービス・サーバによって達成できる。
 【0060】サービス仕様では、クライアントIDはサービス・サーバ506がサービス・クライアント502、520を識別するためにも必要である。同様に、クライアント502、520はサービス・サーバ506を識別するためにサーバIDを必要とする。クライアントIDおよびサーバIDは関連するサービスを提供するサービス・サーバ506が決定して割り当てることができる。サーバIDはクライアント502、520が識別できるある種のサブネット内では一意的である(例えば一意的なインターネット・ホストIPアドレス)。代替的に、一意的なクライアントIDおよびサーバIDはネットワーク機関が割り当てることもできる。サービス・サーバからサービスを利用する必要があるすべてのクライアント502、520はビジネス調整契約の一部として、クライアントID、サービス・サーバID、および認証または暗号化に必要な鍵をそれぞれ取得する必要が

ある。契約はオンラインでいかなる方法でも取得できる。同様に、クライアント/サーバIDは任意の方法でネットワーク・トランスポート・アドレスにマッピングできる。これらは両方とも図6のネットワーク・ミドルウェア504のドメインである。

【0061】サービス仕様ではまたクライアント・コンテキスト・トークンはサービス・サーバ506へのサービス要求（例えば下記の図7ないし図9のサービス要求604を参照）の一部としてサービス・クライアント502、520が提出できる。サービス・サーバ506はサービス要求を処理することで生成される1つまたは複数のサービス・サーバ・イベント内でクライアント・コンテキスト・トークンを再生する。これによってサービス・クライアント502、520はサービス・サーバ・イベントを以前に提出したサービス要求へ関連付けることができる。サービス仕様はトークンの特定のフォーマットを定義しない。トークン・フォーマットはクライアントの私的定義に委ねられ、クライアントによって発行される必要はない。サービス・サーバ506が実行する必要があるのは、それをクライアントのサービス要求を処理した結果として生成される1つまたは複数のサーバ・イベントへ返すことである。クライアント・コンテキスト・トークンの認証はそれを発行したサービス・クライアント502、520の裁量に完全に任されている。例えば、サービス・クライアント502、520は暗号化技術（例えば動的トークン内容データをクライアントにだけ知られた秘密鍵とXORする）を用いてそのクライアント・コンテキスト・トークンの完全性を検査できる。クライアント・コンテキスト・トークンのフォーマットを定義しないことでサービス・クライアントがコンテキスト・トークンの正確さと完全性を自由に検証できるようにする。トークンは発行元によって有効期限切れにされる場合もある（例えばクライアントが応答サービス・サーバ・イベントを待つのを諦めた場合）。

【0062】引き換えクーポンは2つの特定の目的にかなう。第1の目的は、サービス・サーバ506がサービス要求を他の関連するサービス要求（例えば同じトランザクション、同じクライアント）に関連させることを可能にするデータを、サービス・サーバ506がクーポン内に直接または参照により間接的に配置することを許可することである。第2の目的は、サービス・サーバ506がサービス要求を受け入れるための前提条件（例えば以前のサービス要求が首尾よく完了したこと）が揃っているかどうかを判定することを可能にするデータを、サービス・サーバ506が直接または参照により間接的に配置できることである。引き換えクーポンはサービス・サーバ506からのサービス・サーバ・イベントでサーバ・クライアント502、520へ渡される。次に引き換えクーポンはサービス・サーバ506への次に関連するサービス要求の一部として提出される。要求を処理す

るために用いるコンテキストは引き換えクーポンを検査することでサービス・サーバ506によって識別される。

【0063】この仕様は引き換えクーポンのフォーマットを定義しない。引き換えクーポンのフォーマットはサービス・サーバ506の私的定義に委ねられ、サービス・サーバ506によって発行される必要はない。サービス・クライアント502、520が実行する必要があるのはそれをサービス・サーバ506への次のサービス要求に入れることである。引き換えクーポンの認証はそれを発行したサービス・サーバ506の裁量に完全に任されている。例えば、サービス・サーバは暗号化技術（例えば動的コンテンツデータをサービス・サーバにだけ知られた秘密鍵とXORする）を用いてそのクーポンの完全性を検査できる。引き換えクーポンのフォーマットを定義しないことでサービス・サーバ506が引き換えクーポンの正確さと完全性を自由に検証できるようにする。引き換えクーポンは発行元によって有効期限切れにされる場合もある（例えばサービス・サーバがクーポンの宛て先からの次のサービス要求を待つのを諦めてトランザクションを取り消す場合）。

【0064】それぞれのサービス要求は、満たされると引き換えクーポンに反映される、受け入れの前提条件を規定する。したがって、引き換えクーポンは累積的であり、その後に生成されたそれぞれの引き換えクーポンは以前のクーポンが使われずマイレージを累積する。サービス要求前提条件チェック処理は2つのモードで定義および発行できる。第1に、サービス・サーバ506はクライアントのために選択されたサービス・サーバ・イベントを生成できる。これで、サービス・クライアント502、520についての選択されたイベントが以前に発生したことを条件としてサービス要求を受け入れることが可能になる。これらのイベントはクライアント502、520からの以前の選択された1つまたは複数のサービス要求の適切な処理の結果でもよい。第2に、クライアントは以前のイベントで十分なポイントを累積している場合がある。累計ポイントは戻された引き換えクーポンを利用してサービス・サーバ506によって追跡される。引き換えクーポンのフォーマットはクライアント・アプリケーションの開発者へ指示を与えるためにサービス・サーバ506によって発行されてもよい。上記のクーポンの宛て先が得たマイレージはサービス・サーバ506によって引き換えクーポン内に表すことができる。サービス・クライアント502、520が稼いだマイレージはサービス・サーバ506の裁量でリセットされる。

【0065】サービス仕様では、それぞれのサービス要求は専用のデータ要素セットで定義される。また、それぞれのサービス・サーバ・イベント（イベントID）も専用のデータ要素セットで定義される。データ要素は、

10

20

30

40

50

基本の共通基本定義の内容を超えて、サービス・サーバ506とそのクライアント502、520の間でのデータ転送を可能にする。サービス・クライアント502、520があるサービス・サーバからデータ（例えば購入クーポン）を取得し、それをサービス要求に入れて他のサービス・サーバへ渡す必要がある場合、データ要素はそれを行うための手段を提供する。ただしこの場合はデータ要素のフォーマットおよび内容に関して2つのサービス・サーバ間での特殊な調整（例えば2つのサーバ間での専用セキュリティ方式）が必要である。必要に応じて、データ要素の暗号化がサービス・サーバによってサービス仕様内で指定される。サービス・サーバ506は非送信請求サービス・サーバ・イベントを発行することによってサービス・クライアントへ新しい鍵（所定の鍵で暗号化された）を通知することができる。データ要素は実行可能なスクリプトを含めるために用いることができる。このようなデータ要素はデジタル署名の生成に含まれることが多い。

【0066】サービス仕様では、デジタル署名はサービス要求およびサーバ・イベント・メッセージの真正さを確認するのに用いられるのが好ましい。デジタル署名はメッセージのソースを認証し、メッセージの変更を検出し、無許可のサービス・クライアントによる引き換えクーポンの無許可の違法な記録および再生を検出するのに用いられる。

【0067】上述したように、サービス要求は結果として反復イベントを生むことがある。したがって、反復サービス・サーバ・イベント・メッセージが用いられる（例えば、サービス・クライアントからのカード・トランザクション・サービス要求に回答してカード挿入につき1つ）。サービス仕様の前提事項の同期化を保证するため、それぞれのサービス要求の処理の一部として、クライアントが前提とするサービス仕様はサービス・サーバが実際にサポートする内容と比較される。

【0068】サービス仕様では、サービス・クライアント502、520はサービス・サーバ・イベントを待っている間に必要に応じてタイムアウトすると予想される。

【0069】また、サービス仕様には装置またはその機能への直接の参照はない。例えば、ディスプレイ・サービスはサービス・サーバ506が許可する形でディスプレイ装置510を間接的に使用する。これによってサービス要求を実行するために用いる装置510の構成の選択の柔軟性がサービス・サーバ506に提供される。

【0070】サービス仕様では、サービス・サーバ・イベントは物理的イベント（例えば消費者カードの挿入と取り出し）の発生後に初めて発生する。

【0071】サービス仕様は、サービスを要求しサービス要求の処理の結果を取得するためのネットワーク・メッセージ・フォーマットおよびフローを定義しない。し

たがって、サービス・サーバ506とサービス・クライアント502、520の間に通信、ハンドシェーク、保証付き送達などを提供することはミドルウェア504に一任されている。例えば、サービス・サーバ・イベントはミドルウェアが選択した最適化ストラテジを用いてサービス・サーバ506からの非同期メッセージにより通信できる。

【0072】上述したように、サービス・クライアント502（例えばダウンロードされたJavaアプレット）はサービス・サーバ506と同じ端末またはコンピュータ内でローカルに実行できる。

【0073】このように、サービス仕様はメッセージ交換要件の全範囲をカバーしている。しかしながら、他の実施態様ではオプションとしてサービス仕様のサブセットだけを実施することも可能である。例えば、ネットワークが安全な場合にはデータ要素のデジタル署名/暗号化を省略でき、ミドルウェア504がクライアントおよびサーバのルーティングおよび認証を行う場合にはクライアントIDおよびサーバIDを省略できる。

【0074】通信シナリオの例

図7はサービス・クライアント502、520とサービス・サーバ506間の通信の1つのシナリオを示す流れ図である。繰り返すが、サービス・クライアント502は端末上で実行できるダウンロードされたアプレットでもよい。処理はサービス・クライアント502、520がサービス・サーバ506へサービス要求604を送信するステップ602で開始する。サービス要求604はクライアント・コンテキスト・トークン1を含む。サービス・サーバ506はステップ606でサービス要求604に回答する。ステップ606で、サービス要求604はサポートされるサービスおよび対応するサービス仕様に関して確認される。またクライアントも確認/認証され、引き換えクーポンを含むサービス要求メッセージも確認/認証される。サービス要求604が拒否されると、サービス・サーバ拒否イベント608がサービス・サーバ506からサービス・クライアント502、520へ送信される。サービス・サーバ拒否イベント608はクライアント・コンテキスト・トークン1を再生し、サービス・サーバ506の処理を終了する。そうでない場合、すなわちサービス要求がサービス・サーバ506によって受け入れられた場合、処理はステップ610に進む。ステップ610で、コンテキストがサービス要求604から取り出される。このステップで、必要に応じて操作案内および対話が提供され、端末装置に関して複数の非同期動作が実行される。サービス・サーバ506は次にサービス・クライアント502、520へサービス・サーバ・イベント（送信請求）612を送信する。サービス・サーバ・イベント612は引き換えクーポンAを含み、クライアント・コンテキスト・トークン1を再生する。サービス・サーバ・イベント（送信請求）6

12は単一イベント、複数イベント、または反復イベントである。サービス・クライアント502、520はサービス・サーバ・イベント612を受信すると、ステップ614でサーバIDおよびクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを確認/認証し、さらなるサービス要求616をサービス・サーバ506へ送信する。このさらなるサービス要求616はクライアント・コンテキスト・トークン2を含み、引き換えクーポンAを再生する。

【0075】通信処理はステップ606および610にしたがって第1のサービス要求604のときと同様に続行する。

【0076】図8にサービス・サーバ506とサービス・クライアント502、520間のメッセージ・シナリオの第2の例を示す。処理はサービス・サーバ506がサービス・クライアント502、520にサービス・サーバ・イベント654を送信するステップ652で開始する。サービス・サーバ・イベント（非送信請求）654は引き換えクーポンBを含む。サービス・クライアント502、520がサービス・サーバ・イベント654を受信すると、サービス要求658がステップ656でサービス・サーバ506へ送信される。サービス要求658はクライアント・コンテキスト・トークン3を含み、引き換えクーポンBを再生する。ステップ660で、サービス・サーバ506はサポートされるサービスおよび対応するサービス仕様に関してサービス要求を確認し、クライアントおよび引き換えクーポンを含むサービス要求メッセージを確認/認証する。サービス要求がサービス・サーバ506により拒否される場合、サービス・サーバ拒否イベント662がサービス・クライアント502、520へ送信され、サービス・クライアント502、520はクライアント・コンテキスト・トークン3を再生する。そうでない場合、サービス・サーバ506の処理はステップ664に進む。ステップ664で、コンテキストが取り出され、必要に応じて操作案内および対話と非同期動作が実行される。サービス・サーバ506は次にサービス・クライアント502、520へサービス・サーバ・イベント（送信請求）666を送信する。サービス・サーバ・イベント666は引き換えクーポンCを含み、クライアント・コンテキスト・トークン3を再生する。サービス・クライアント502、520はサーバIDおよびクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを確認/認証し、ステップ668でサービス・サーバ506へサービス要求670を送信する。このさらなるサービス要求670はクライアント・コンテキスト・トークン4を含み、引き換えクーポンCを再生する。

【0077】図9にサービス・サーバ506とサービス・クライアント502、520間のメッセージ・シナリオの第3の例を示す。サービス・サーバ506はステッ

プ672でサービス・クライアントへ非送信請求サービス・サーバ・イベントを送信する。サービス・サーバ・イベント（非送信請求）674はサーバ状況メッセージ、随通知メッセージなどで、引き換えクーポンを値えることができる。

【0078】ミドルウェア504はメッセージの完全性、同期化、保証付きメッセージ送達などのために図7ないし図9のシナリオのメッセージの上にさらにメッセージを構築することができ、また同じ情報を異なるフォーマットで表すこともできる。

【0079】サービス・サーバ内のサービス要求の処理図10および図11はサーバ506内のサービス要求の処理の例を示す流れ図である。処理はステップ700で開始する。ステップ702で、次のサービス要求がクライアントまたは内部ジョブ待ち行列から取得される。後者の場合、内部待ち行列からの内部的に生成されたサービス要求が非送信請求サーバ・イベントを生成する。判断ブロック704で、クライアントが有効かどうかを判定するためのチェックがなされる。クライアントが有効でなければ、拒否イベントがステップ706で通知される。そうでない場合、処理は判断ブロック708に進む。判断ブロック708で、引き換えクーポンを含むサービス要求が有効か、また変更されていないか（すなわちソースが有効かなど）を判定するためのチェックがなされる。デジタル署名があればここで使用される。判定の結果有効でなければ、拒否イベントがステップ710で通知される。そうでない場合、処理は判断ブロック712に進む。判断ブロック712で、引き換えクーポンが有効かどうかを判定するためのチェックがなされる。これはコンテキストIDの突き合わせ、同じコンテキストを有する別のサービス要求が処理中であるかどうかのチェックを含む。問題なければ、引き換えクーポンがそのサービス要求に許されるかどうかを判定するためのチェックがなされる。また前提条件が満たされているかどうかを判定するためのチェックもなされる。判定結果がノーであれば、処理はステップ714に進み、拒否イベントが通知される。さもなければ、処理はステップ716に進む。ステップ716で、サービス要求メッセージの残りが分解される。これはサービス要求データ要素の抽出、選択したデータ要素の非暗号化、およびクライアント・コンテキスト・トークンがあればその保存を含む。処理は次に判断ブロック718に進む。

【0080】判断ブロック718で、サービス要求が既存のコンテキストの一部であるかどうかを判定するためのチェックがなされる。判定結果がイエスであれば、処理はステップ724に進む。ステップ724で、コンテキスト制御ブロックが取り出される。処理は次にステップ726に進む。そうでない場合、すなわち判断ブロック718がノーを返した場合、処理は判断ブロック720に進む。判断ブロック720で、必要な1つまたは複

数の資源が利用できるかどうかを判定するためのチェックがなされる。利用可能でなければ、処理はステップ722に進み、イベントが通知される。されなければ、処理はステップ726に進む。

【0081】ステップ726で、サービス要求に固有の処理がサービス要求状態に関して実行される。操作案内および対話が必要に応じて提供される。処理は次に判断ブロック728に進む。判断ブロック728で、これが新しいコンテキストであるかどうかを判定するためのチェックがなされる。新しいコンテキストであれば、処理はステップ730に進む。ステップ730で、クーポンに対して新しいコンテキストIDが割り当てられ、新しいコンテキスト制御ブロックが作成される。処理は次に判断ブロック732に進む。そうでない場合、すなわち判断ブロック728がノーを返した場合、処理は判断ブロック732に進む。

【0082】判断ブロック732で、クライアントのための引き換えクーポンがあるかどうかを判定するためのチェックがなされる。判定結果がノーであれば、処理はステップ736に進み、さもなければ、ステップ734に進む。ステップ734で、引き換えクーポンが作成される。処理は次にステップ736に進む。

【0083】ステップ736でイベント・メッセージが組み立てられる。ステップ738で、サービス・サーバ・イベントが通知される。判断ブロック740で、そのサービス要求についての処理が終了したかどうかを判定するためのチェックがなされる。まだであれば、処理はステップ726に戻る。

【0084】終了の場合は、処理は判断ブロック742に進む。判断ブロック742で、コンテキストの終りまで到達したかどうかを判定するためのチェックがなされる。判定結果がイエスであれば、処理はステップ744に進む。ステップ744で、コンテキスト制御ブロックが削除される。処理は次にステップ746に進む。コンテキストの終りに達していなければ、処理はステップ748に進む。ステップ748で、コンテキスト制御ブロックが保存される。処理は次にステップ746に進む。ステップ746で、サービス要求の処理は終了する。

【0085】サービス・クライアントでのサービス・サーバ・イベントの処理

図12はサービス・クライアントでのサービス・サーバ・イベントの処理の例を示す流れ図である。処理はステップ800で開始する。ステップ802で、次のサービス・サーバ・イベントがサービス・サーバから取得される。判断ブロック804で、サービス・サーバが有効かどうかを判定するためのチェックがなされる。サービス・サーバが有効でなければ、エラー処理がステップ806で実行される。さもなければ、処理は判断ブロック808に進む。判断ブロック808で、サーバ・イベントが有効かどうかを判定するためのチェックがなされる。

このチェックはクライアント・コンテキスト・トークンを含むイベント・メッセージが有効か、また変更されていないか、ソースが認証されているかなどを判定するためのチェックを含む。デジタル署名があればここで使用される。判定結果がノーであれば、エラー処理がステップ810で実行される。さもなければ、処理は判断ブロック812に進む。

【0086】判断ブロック812で、サービス・サーバ・イベントが非送信請求かどうかを判定するためのチェックがなされる。非送信請求であれば、処理は判断ブロック816に進み、さもなければステップ814に進む。ステップ814で、コンテキストがクライアント・コンテキスト・トークンを用いて取り出される。処理は次に判断ブロック816に進む。

【0087】判断ブロック816で、引き換えクーポンが利用可能かどうかを判定するためのチェックがなされる。すなわち、サービス・クライアントがサービス・サーバで以降の引き換えに利用できるクーポンがあるかどうかを判定するためのチェックがなされる。利用可能であれば、処理はステップ818に進む。ステップ818で、引き換えクーポンが後で使用するために保存される。処理は次にステップ820に進む。引き換えクーポンが利用可能でなければ、処理はステップ820に進む。ステップ820で、イベントが処理される。これはイベント・データ要素の抽出とそれから選択した要素の非暗号化を含む。処理は次に判断ブロック822に進む。

【0088】判断ブロック822で、次のサービス要求をサービス・サーバへ出すかどうかを判定するためのチェックがなされる。出さないのであれば、処理は判断ブロック826に進み、さもなければステップ824に進む。ステップ824で、新しいクライアント・コンテキスト・トークンが作成され、サービス要求がサービス・サーバへ送られる。これはクライアント・コンテキスト・トークンの生成、データ要素の組立て（選択したデータ要素の暗号化を含む）、以前に保存された引き換えクーポンの取得、およびデジタル署名の構築を含み得る。処理は次に判断ブロック826に進む。

【0089】判断ブロック826で、サービス・サーバ・イベントが非送信請求かどうかを判定するためのチェックがなされる。非送信請求であれば、処理はステップ830に進み、さもなければステップ828に進む。ステップ828で、処理されたサービス・サーバ・イベントに関連付けられていた既存のクライアント・コンテキストが削除され、処理は次にステップ830に進む。ステップ830でイベントの処理は終了する。

【0090】

【0091】

【図面の簡単な説明】

【図1】いくつかの従来のホスト・コンピュータおよび

31

端末構成を示すブロック図である。

【図2】いくつかの従来のホスト・コンピュータおよび端末構成を示すブロック図である。

【図3】それぞれ関連する端末ネットワークを備えたいくつかのホスト・コンピュータ間の通信を示すブロック図である。

【図4】いくつかのホスト・コンピュータ間での組織間通信を示すブロック図である。

【図5】本発明の好ましい実施形態によるサービス・サーバとサービス・クライアントの間の通信を可能にする公衆ネットワークを示すブロック図である。

【図6】好ましい実施形態によるネットワークのサービス・サーバとリモート・クライアントを示すブロック図である。

*

32

*【図7】第1のシナリオの図6のサービス・サーバとサービス・クライアントの間のメッセージ伝送を示す流れ図である。

【図8】第2のシナリオのメッセージ伝送を示す流れ図である。

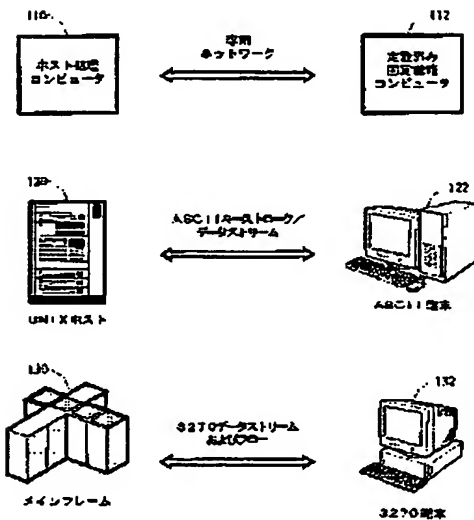
【図9】第3のシナリオのメッセージ伝送を示す流れ図である。

【図10】図6のサービス・サーバのサービス要求の処理を示す流れ図である。

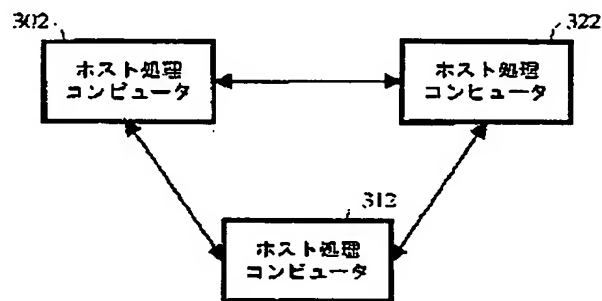
【図11】図6のサービス・サーバのサービス要求の処理を示す流れ図である。

【図12】図6のサービス・クライアントのサービス・サーバ・イベントの処理を示す流れ図である。

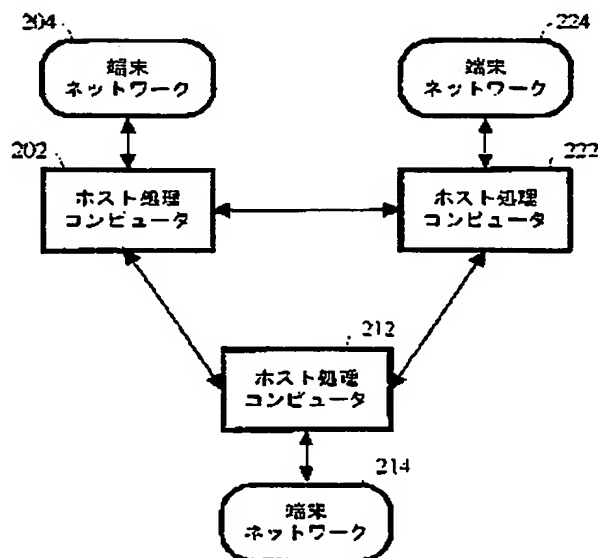
【図1】



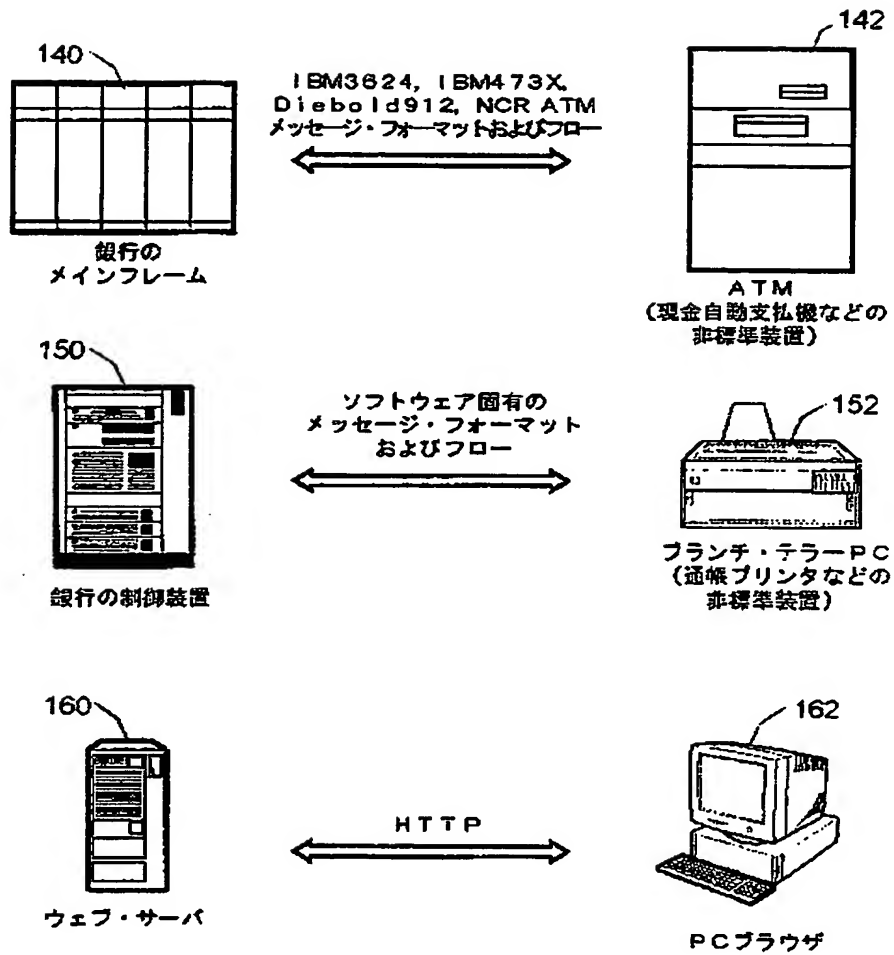
【図4】



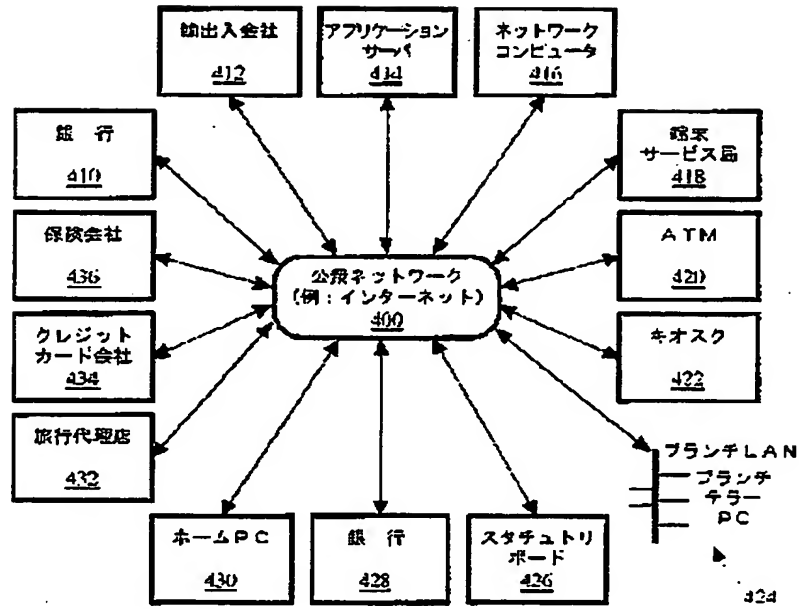
【図3】



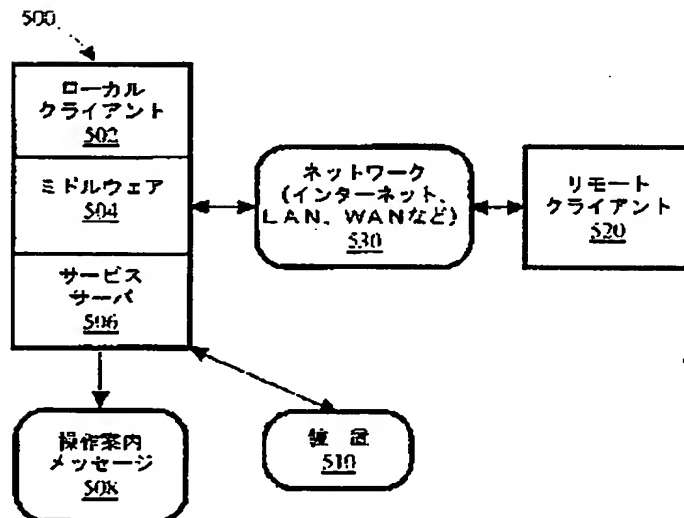
【図2】



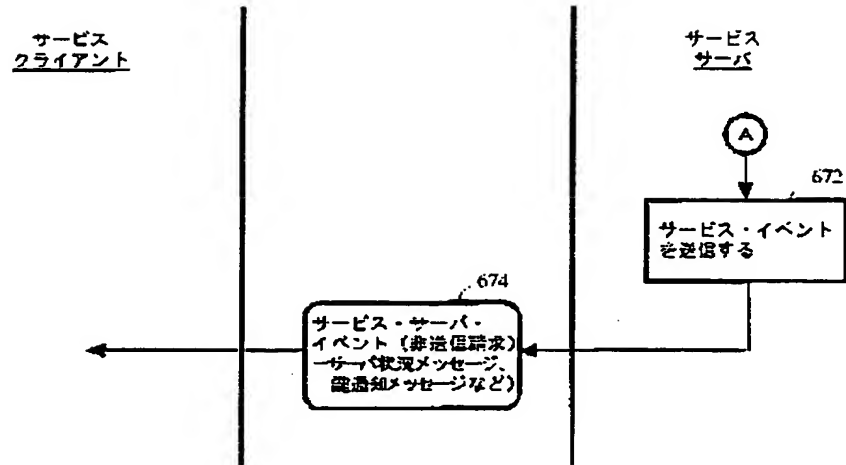
【図5】



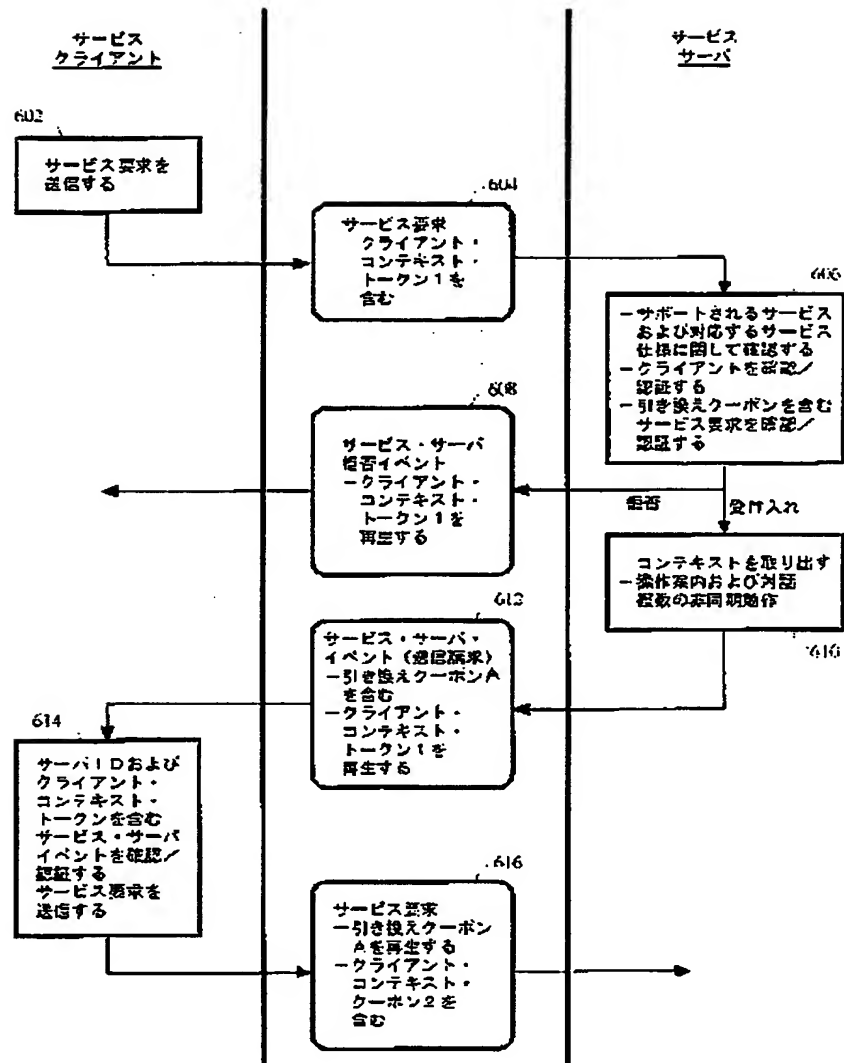
【図6】



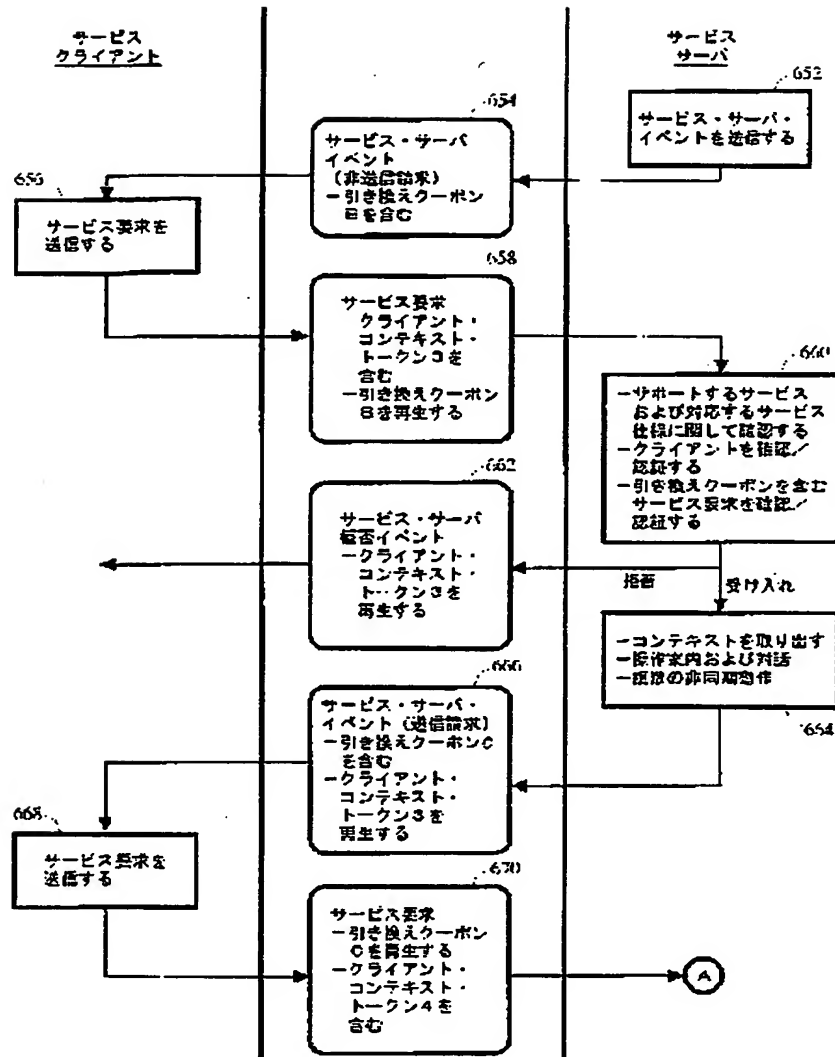
【図9】



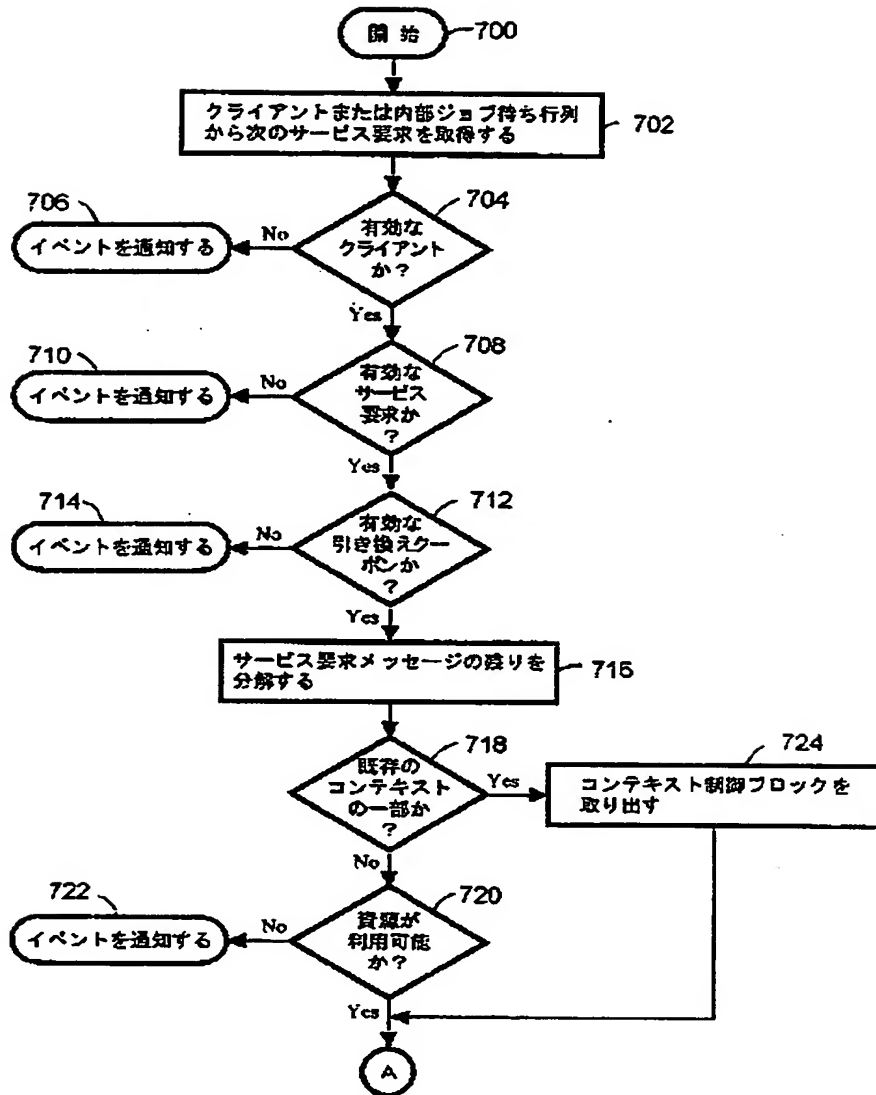
【図7】



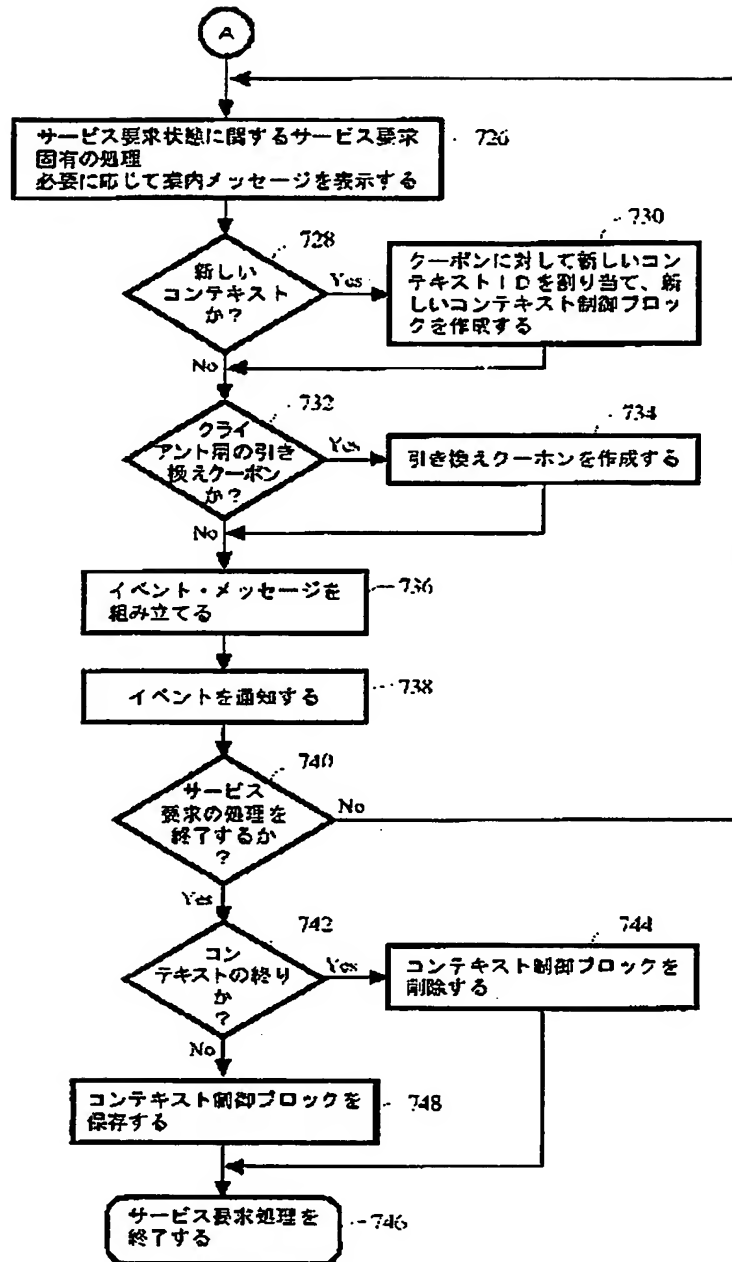
【図8】



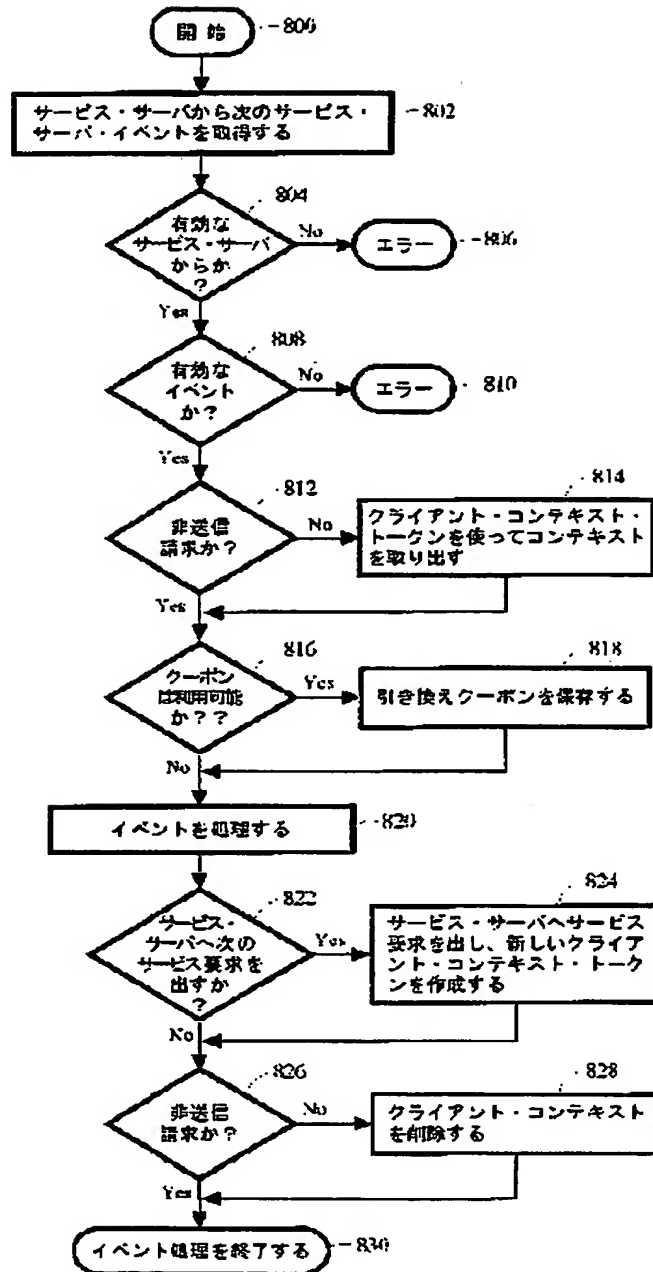
【図10】



【図11】



【図12】



フロントページの続き

(56)参考文献 国際公開97/23838 (WO, A1)
Goldstein, T., "The
Gateway Security
Model in the Java
Electronic Commerce
Framework", Lecture
Notes in Computer
Science, Feb. 1997,
No. 1318, p. 340-354

(58)調査した分野(Int.Cl.⁷, DB名)

G06F 17/60 324

G06F 17/60 410

G06F 17/60 502

G06F 13/00 357

JICSTファイル(JOIS)